

GOVERNANCE DOCS

CIS Controls v8.1

Gap Assessment Report

CIS Critical Security Controls Version 8.1

Maple Street Accounting (sample)

The firm's office network, laptops, Microsoft 365 tenant and client file storage.

ASSESSED	25 September 2026
EDITION	Version 8.1, published 25 June 2024
IN SCOPE	66 requirements, 64 applicable
PROFILE	Professional services · 10 to 49 people
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Maple Street Accounting (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Maple Street Accounting (sample) stands against CIS Controls



APPLICABLE	EVIDENCED	OPEN GAPS	HIGH PRIORITY
64	22	42	16

STATUS OF EVERY REQUIREMENT



Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced
Not applicable

GAPS WITH AN OWNER	WITH A TARGET DATE	NOT ANSWERED
21 of 42	13 of 42	0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 63.3% against CIS Controls across 64 applicable controls. 22 of them are implemented and evidenced.
- Most open gaps: Controls 9-13 - Technical defences, with 12 at 37%. Strongest area: Controls 14-16 - People, suppliers and software at 95%.
- 13 controls are operating but not evidenced. Collecting their records alone lifts the score to 68.4% (+5.1 points), the cheapest gain available.
- 16 gaps are high priority (not started or only planned); 7 of them are in Controls 9-13 - Technical defences.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 7 high-priority gaps in Controls 9-13 - Technical defences	Compliance Lead	
2	LOW	Evidence the 13 controls that already operate (+5.1 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

Your readiness score is 63.3% at Developing level; focus immediately on closing 16 high priority technical and response gaps.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

The organization has attained a 63.3% score under the CIS Controls v8.1 self-assessment, placing us at the Developing stage. While personnel and supplier controls are robust, our primary vulnerabilities sit in technical defences and incident response, which scored 36.5% and 40% respectively. To mitigate potential disruption, leadership must approve target dates and designate owners for all 42 open gaps. Management requests board backing to prioritize technical remediation, automated backups, and formal incident testing over the next 90 days.

WHERE YOU STAND

The self-assessment places the organization at a Developing readiness level with an overall score of 63.3%. Across 64 applicable requirements, you have 22 implemented and evidenced, while 42 open gaps remain. Of these open items, 16 are high priority. A significant portion of your programme already operates, including 13 items implemented without evidence and 13 partially implemented items. However, only 21 gaps have an assigned owner, and 13 have a target completion date. Addressing these unassigned gaps is necessary to establish accountability across the remaining controls.

WHAT IT MEANS FOR THE ORGANIZATION

The distribution of scores reveals a clear divide between administrative controls and core operational defences. Controls 14-16 - People, suppliers and software scores highest at 95.5%, demonstrating mature governance around personnel and vendors. Conversely, technical safeguards show severe deficiencies. Controls 9-13 - Technical defences scored 36.5% with 12 open gaps, while Controls 17-18 - Response and testing reached only 40%. Without solid technical defences and incident readiness, the organization faces substantial exposure during operational disruptions or direct cyber attacks, leaving critical business systems and recovery procedures vulnerable.

WHERE TO FOCUS FIRST

Immediate efforts must target unstarted and planned high priority safeguards. First, formalise incident handling through Incident response foundations and Plan, roles and communication to ensure readiness during emergencies. Second, protect critical assets by addressing Recovery process and automated backups and Remediate detected vulnerabilities. Finally, convert existing operational practices into validated controls by gathering documentation for the 13 items currently implemented without evidence. Evidencing these operational practices alone increases the assessment score from 63.3% to 68.4% before completing partially implemented controls.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Establish Incident Response Capabilities 17.1-17.3 Incident response foundations · 17.4-17.6 Plan, roles and communication	Without defined response plans and designated roles, cyber incidents can cause uncoordinated reactions and prolonged business downtime.	Draft core communication protocols and assign primary roles for incident handling.	Comprehensive CIS Controls v8.1 Toolkit - 40 Cybersecurity Templates	30 DAYS
2 Secure and Validate Business Backup Systems 11.1-11.2 Recovery process and automated backups · 11.3-11.4 Protect and isolate recovery data · 11.5 Test recovery	Incomplete backup isolation and untested recovery expose the business to catastrophic data loss during ransomware attacks or system outages.	Verify automated backup schedules and isolate secondary recovery data off the primary network.	Comprehensive CIS Controls v8.1 Toolkit - 40 Cybersecurity Templates	30 DAYS
3 Remediate Vulnerabilities and Standardise System Logging 7.7 Remediate detected vulnerabilities · 8.4-8.8 Time synchronisation and detailed logging	Failing to remediate detected vulnerabilities and maintain synchronised logs hinders threat detection and leaves known entry points open.	Configure system clocks across servers and schedule patches for identified high severity vulnerabilities.	Comprehensive CIS Controls v8.1 Toolkit - 40 Cybersecurity Templates	60 DAYS
4 Complete Enterprise Asset and Software Inventories 1.1 Enterprise asset inventory · 1.2 Unauthorised assets	Uncontrolled devices and software introduce unmonitored risk vectors across the internal corporate environment.	Consolidate active network device records into an authoritative asset register.	Comprehensive CIS Controls v8.1 Toolkit - 40 Cybersecurity Templates	60 DAYS
5 Conduct Validation and Internal Security Testing 18.4-18.5 Validation and internal testing	Untested controls create false confidence and leave technical weaknesses undiscovered until an external breach occurs.	Define a testing scope and schedule for internal technical control validation.	Comprehensive CIS Controls v8.1 Toolkit - 40 Cybersecurity Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Assign owners and definitive completion dates to all 42 open gaps.
- Draft foundational incident response procedures, roles, and emergency communication paths.
- Verify automated backup execution and isolate secondary recovery data.
- Collect required documentation for the 13 controls currently implemented without evidence.

DAYS 31 TO 60

- Establish formal patch management schedules to remediate detected system vulnerabilities.
- Implement network time synchronisation and enable centralized logging for critical systems.
- Finalise the enterprise asset inventory and establish rules for unauthorised assets.

DAYS 61 TO 90

- Conduct an end-to-end data restoration test from isolated backup media.
- Execute internal validation testing to assess technical security controls.
- Complete outstanding implementation work on the 13 partially implemented controls.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Controls 1-2 - Know what you have		67%	
Control 3 - Data protection		72%	
Control 4 - Secure configuration		70%	
Controls 5-6 - Accounts and access		72%	
Controls 7-8 - Vulnerabilities and logs		53%	
Controls 9-13 - Technical defences		37%	
Controls 14-16 - People, suppliers and software		95%	
Controls 17-18 - Response and testing		40%	

■ Not started
 ■ Planned
 ■ Partially implemented
 ■ Implemented, not evidenced
 ■ Implemented and evidenced
 ■ Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today		63.3%
Evidence what already runs 13 requirements		68.4% +5.1
Finish what is partly in place 13 requirements		78.5% +10.1
Implement what is planned 9 requirements		89.1% +10.6
Start what has not begun 7 requirements		100.0% +10.9

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

All of these are in the CIS Controls Toolkit (40 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 7

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
7.7	Remediate detected vulnerabilities	Controls 7-8 - Vulnerabilities and logs	To assign	
8.4-8.8	Time synchronisation and detailed logging	Controls 7-8 - Vulnerabilities and logs	HR Manager	
9.3-9.7	Email and web hardening	Controls 9-13 - Technical defences	Compliance Lead 21 Jan 2027	
11.1-11.2	Recovery process and automated backups	Controls 9-13 - Technical defences	Operations Manager 10 Dec 2026	
12.1	Network infrastructure currency	Controls 9-13 - Technical defences	Compliance Lead 12 Nov 2026	
13.1-13.3	Alerting and intrusion detection	Controls 9-13 - Technical defences	HR Manager	
18.4-18.5	Validation and internal testing	Controls 17-18 - Response and testing	To assign	

HIGH Planned · 9

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
1.1	Enterprise asset inventory	Controls 1-2 - Know what you have	Operations Manager 12 Nov 2026	
1.2	Unauthorised assets	Controls 1-2 - Know what you have	IT Manager	
4.3-4.5	Session locking and host firewalls	Control 4	To assign	
5.2-5.3	Unique passwords and dormant accounts	Controls 5-6 - Accounts and access	Compliance Lead 12 Nov 2026	
10.4-10.6	Centralised and automated malware defence	Controls 9-13 - Technical defences	Risk Manager 26 Nov 2026	
11.3-11.4	Protect and isolate recovery data	Controls 9-13 - Technical defences	To assign	

11.5	Test recovery	Controls 9-13 - Technical defences	IT Manager 4 Feb 2027
17.1-17.3	Incident response foundations	Controls 17-18 - Response and testing	To assign
17.4-17.6	Plan, roles and communication	Controls 17-18 - Response and testing	IT Manager

MEDIUM Partially implemented · 13

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
3.4-3.5	Retention and disposal	Control 3	HR Manager 10 Dec 2026	
3.7	Data classification scheme	Control 3	To assign	
3.10-3.11	Encryption in transit and at rest	Control 3	Compliance Lead 7 Jan 2027	
4.10-4.12	Portable device controls	Control 4	Compliance Lead	
5.4-5.5	Administrator and service accounts	Controls 5-6 - Accounts and access	To assign	
6.1-6.2	Access granting and revoking processes	Controls 5-6 - Accounts and access	Compliance Lead 26 Nov 2026	
7.1-7.2	Vulnerability and remediation processes	Controls 7-8 - Vulnerabilities and logs	Risk Manager 7 Jan 2027	
7.5-7.6	Vulnerability scanning	Controls 7-8 - Vulnerabilities and logs	HR Manager 7 Jan 2027	
8.2-8.3	Collect logs and provide storage	Controls 7-8 - Vulnerabilities and logs	HR Manager	
9.1-9.2	Supported browsers and DNS filtering	Controls 9-13 - Technical defences	Operations Manager	
12.5-12.8	Centralised AAA and privileged access paths	Controls 9-13 - Technical defences	HR Manager 21 Jan 2027	
13.4-13.6	Segmentation and traffic visibility	Controls 9-13 - Technical defences	To assign	
15.5-15.7	Assess, monitor and decommission	Controls 14-16 - People, suppliers and software	Compliance Lead	

LOW Implemented, not evidenced · 13

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
-----	-------------	------	----------------	-----------

1.3-1.5	Discovery tooling	Controls 1-2 - Know what you have	To assign
2.2	Supported software only	Controls 1-2 - Know what you have	To assign
3.1	Data management process	Control 3	To assign
3.3	Data access control lists	Control 3	To assign
3.6-3.9	Encryption on devices and media	Control 3	To assign
4.1-4.2	Secure configuration process	Control 4	To assign
5.6	Centralised account management	Controls 5-6 - Accounts and access	To assign
6.6-6.7	Authentication inventory and centralised access control	Controls 5-6 - Accounts and access	To assign
8.12	Service provider logs	Controls 7-8 - Vulnerabilities and logs	To assign
10.1-10.3	Anti-malware basics	Controls 9-13 - Technical defences	To assign
13.7-13.11	Prevention and tuning	Controls 9-13 - Technical defences	To assign
17.7-17.9	Exercises, reviews and thresholds	Controls 17-18 - Response and testing	To assign
18.1-18.3	Penetration testing programme	Controls 17-18 - Response and testing	To assign

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com